Issues of Migration from IPv4 to IPv6

Gjorgi Mikarovski[1], Aleksandar Kotevski[2], Ilija Jolevski[3]

Abstract – **Internet Protocol (IP) has become the standard communication tool, ever since its introduction in 1970's. This resulted inmajortechnological developments of the internetworking devices. IPv6 is a new version of Internet Protocol, developed by the Internet Engineering Task force (IETF) as an evolutionary step from IPv4. The most important purpose of IPv6 is to allow a greater number of connected hosts than allowed by IPv4. While IPv4 allows 32 bits for an Internet Protocol address, and can therefore support 232 (4,294,967,296) addresses, IPv6 uses 128-bit addresses, so the new address space supports 2128 (approximately 340 undecillion or 3.4×1038) addresses. In addition, IPv6 reduces packet processing overhead and increases scalability. Together, these improvements allow a greater exchange of data traffic.**

Keywords – **communication, traffic, network, protocol, migrations, dual-stack, tunnelling, IP/ICMP, NAT-PT, 6 to 4, 4 over 6.**

I. INTRODUCTION

IETF designed IPv6 to allow interoperability between devices that use the IPv4 stack and devices that use the IPv6 stack. It is usually possible to install IPv6 on internet devices without losing IPv4 capability, so organizations can perform incremental upgrades from IPv4 to IPv6 while avoiding disruption of service during the transition.

Since IPv4 and IPv6 packets are not directly compatible, therefore a technique known as translators are used that translate the IPv4 packets into IPv6 and vice versa. But translators tend to slow the network. Translation between IPv4 and IPv6 can take place at three levels i.e. IP level, transport level and the application level.

II. OVERVIEW OF IPV4 AND IPV6

The IPv4 addresses are represented with dot decimal notation. The addresses are divided into two parts, the network ID and the host ID. The network ID is of 8 bits, therefore it can addresses up to 256 hosts. To overcome this limit, five different classes namely A, B, C, D & E were created and were named as classful addressing. Classless Inter Domain Routing (CIDR) replaced the classful addressing, which allowed the re-division of class A, B & C networks. Class A, B & Care reserved for use by private networks.

[1]Gjorgi Mikarovski is with the Faculty of Technical Science, Ivo Lola Ribar bb 7000 Bitola Macedonia, E-mail: gjorgi.mikarovski@tfb.uklo.edu.mk

[2]Aleksandar Kotevski is with the Faculty of Technical Science, Ivo Lola Ribar bb 7000 Bitola Macedonia, E-mail: aleksandar.kotevski@uklo.edu.mk

[3]Ilija Jolevski is with the Faculty of Technical Science, Ivo Lola Ribar bb 7000 Bitola Macedonia, E-mail: ilija.jolevski@uklo.edu.mk

On the contrary, IPv6 is designed to overcome the deficiencies of IPv4 by expanding the available IP's pool and by incorporating features such as IPsec, quality of service (QOS), efficient routing and mobile communications. These new features can be used to develop new E-Commerce businesses, increase broadband penetration and to enhance the mobile communication.

The transition from IPv4 to IPv6 will take place in three stages i.e. substitution, diffusion and complete transformation. In substitution IPv6 will substitute the IPv4. In this phase organizations implementing IPv6 in their infrastructure will operate in a dual stack environment. In diffusion, new applications will be developed using IPv6 that will be more innovative and economical. In diffusion,IPv4 will be obsolete and new hardware will run entirely on IPv6. The complete transition from IPv4 to IPv6 is expected to take many years.

IPv6 deployment issues

- IPv4 and IPv6 do not interoperate
  - IPv4 applications do not work with IPv6
  - IPv4 nodes cannot communicate with IPv6 nodes
- The applications have to be modified
  - a lot of work still has to be done.
- It is likely that IPv4 and IPv6 will coexistfor a long period of time
  - How to enable communications among IPv6islands isolated in the IPv4 world?
  - How to enable communications between the existing IPv4 world and the new IPv6 world?

III. MIGRATION MECHANISMS

In order to replace the IPv4 protocol, a few years ago the IPv6 protocol has been intro-duced to the internet community. However, IPv4 is still dominating most of the internet infrastructure. We expect that the migration between both protocols will not take place in a rapid way, especially not in the U.S. and Europe. Due to the serious lack of IP addresses in Asia there is more need for IPv6, that's why the migration process will be faster in that region.

The migration mechanisms described in this report are based on the transition. These are: Dual IP layer operation, Tunneling, IPv4-compatible IPv6 addresses, 6to4, 6over4.

Furthermore, there exist other transition mechanisms. Network manufacturers have deployed various proprietary mechanisms, like the Intra Site Automatic Tunnel Addressing Protocol (ISATAP).

Dual IP Layer operation - the most used migration approach nowadays is the dual IP layer operation, also called the dual stack method. A host with a dual stack can interoperate with both IPv4 and IPv6 nodes using IPv4 or IPv6 packets. Dual

stack has the possibility to disable one of the IP stacks for operational reasons. A node configured with a dual stack can make decisions on TCP connections based on the IP header of the TCP packet:

- The IPv4 protocol stack will be used if the destination address used by the application is an IPv4 address;
- The IPv6 protocol stack will be used if the destination address used by the applications an IPv6 address;
- Encapsulation of an IPv6 packet inside an IPv4 packet will occur if the destination address used by the application is an IPv6 address with embedded IPv4 address.

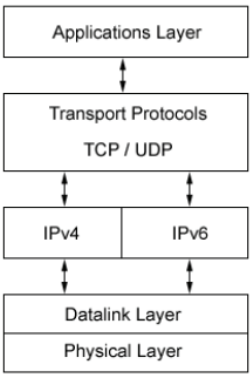

Fig 1. The dual stack approach

Dual stack makes it possible to continue provide access to IPv4 resources, while adding IPv6 functionality. The IP address acquisition in the dual stack nodes occurs by using IPv4 mechanisms like DHCP or IPv6 mechanisms, as for instance the stateless address auto-configuration. Hosts and routers that support dual stack may use tunneling mechanisms to route IPv6 tra c over IPv4 networks.

Issues with simple dual-stack

- it does not reduce the demand for globally routable IPv4 addresses
- it increases network complexity due to the need for a double (IPv4/IPv6) routing infrastructure

Other dual-stack approaches

DSTM (Dual Stack Transition Mechanism)

- deployment of dual-stack nodes with dynamically assigned IPv4 addresses
- IPv4 over IPv6 tunneling to avoid the need for a dual-stack routing infrastructure

Application Level Gateways (ALG)

- the client is IPv6-only and the communication with the IPv4 world goes through a dual-stack proxy

A dual-stack alternative is NAT-PT (NAT - Protocol Translator)

Tunneling - because IPv6 will be developed over the IPv4 infrastructure, tunneling provides a way to use the existing routing infrastructure to carry IPv6 tra c. Tunneling IPv6 packets over IPv4 infrastructure is done by encapsulating IPv6 packets inside IPv4 packets as shown in figure 2. The IPv6 header contains the address of the final destination and the IPv4 header contains the address of the tunnel endpoint. The encapsulation of IPv6 packets within IPv4 packets can occur in the following ways:

Router-to-Router: An IPv4 infrastructure will tunnel IPv6 traffc between directly linked IPv6/IPv4 routers.

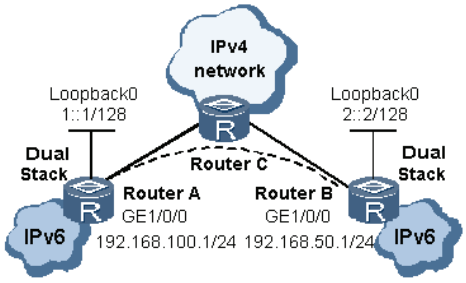

Fig 2. Router to router

Host to Router: IPv6/IPv4 hosts will tunnel IPv6 tra c to an IPv6/IPv4 router via an IPv4 infrastructure.

Fig 3. Host to router

Tunneling of IPv6 over IPv4 - these are amongst the most basic techniques that can be deployed in order to allow operation of two or more protocols on the network. This technique involves the encapsulation of IPv6 packets with in IPv4 header. A tunnel is a link between two IPv4 end points that must be configured by specifyingthe IPv6 destinations for which the packets are to be encapsulated, and the remote IPv4 end point to which they must be sent.

Issues with simple tunneling

- configured tunneling requires heavy manual configuration and therefore does not scale well
- automatic tunneling is not the solution because it can be used only between individual hosts

IPv4-compatible IPv6 - are also known as 6over4. In this mechanism, ex addresses are used to create IPv4-compatible IPv6 addresses. These addresses are by a 96bit zeros prefix followed by the 32bits IPv4 address. In this approach, IPv4 addresses become a virtual link-layer address by using I cast group. Neighbor Discovery takes place by mapping IPv6 multicast address multicast addresses. The router must be configured as 6over4 in order to make IPv routing possible. The hard requirements and poor scalability characterize this implementation.

6 to 4 - It is a method of constructing the IPv6 address directly from the IPv4 address. This mechanism enables sites to communicate over the IPv4 Internet without using explicit tunnels while still communicating with IPv6 relay routers. 6 to 4 treats IPv4 Internet as a unicast point-to-point link layer and specify an encapsulation mechanism for transmitting IPv6 packets using the prefix. This mechanism is implemented entirely in border routers and is thus becoming a

standard feature of router software. Below is thediagram given for 6 to 4

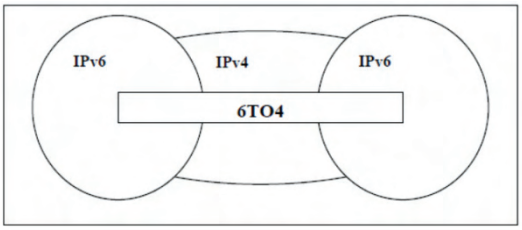

Fig 4. 6to4

6 over 4 - This mechanism facilitates IPv6 connectivitywith in a site that lacks any IPv6 infrastructure. It describes the frame format for IPv6 packets as well as method of forming IPv6 link local addresses over IPv4 multicast domains. It allows IPv6 hosts to become functional if at least one IPv6 router is located in the same domain. This technique is helpful for sites that still have no IPv6 networks but wish to deploy it or test it. 6 over 4 have received very limited support from the major vendors; only Microsoft and Nokia have implementations of 6 over 4.

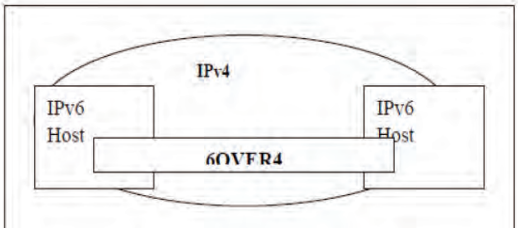

Fig 5. 6over4

IV. TRANSLATION MECHANISMS

Once an IPv4 network connects to an IPv6 network, there is still the need to communicate between the IPv6-only nodes with the IPv4 nodes that are not yet IPv6 enabled. There are various translation mechanisms developed that enable cross-protocol communication. The difference between all the translation mechanisms is where the translation actually takes place in the various layers of the TCP (or UDP)/IP reference model.The different translation mechanisms that we describe in this report, and also have been proposed as a RFC to the IETF are categorized as follows.

*Network layer:*Stateless IP/ICMP Translation Algorithm (SIIT), NAT-PT
*Transport layer:*Transport Relay Translator (TRT)
*Application layer:*Bump in the API (BIA)

Stateless IP/ICMP Translation Algorithm - the stateless IP/ICMP translation algorithm (SIIT) can be used in the transition between IPv4 and IPv6. There are two types of translation:

IPv4 to IPv6 translation
When an IPv4-only node sends a packet to another node, whose destination is an IPv6 ad-dress in another network, the SIIT algorithm detects this. The SIIT algorithm translates the IPv4 header of the packet to an IPv6 header, and discards the IPv4 header. Subsequently the packet is forwarded to the destination IPv6 address. The noticeable dierences between the IPv4 and IPv6 header are in the following fields:

Source field The IPv4 address source address of the IPv4 host is converted to an IPv6 address where the low-order 32 bits is the IPv4 source address. The high-order 96 bits is the IPv4-mapped prefix (::ffff:0:0/96).

*Destination field*the destination address in the IPv4 header is converted to an IPv6 address where the low-order 32 bits is the IPv4 destination address. The high-order 96 bits is the IPv4-translated prefix (::ffff:0:0:0/96).

IPv6 to IPv4 translation
In this translation type, the IPv6 header is translated to IPv4, and the packet is forwarded through IPv4. The issue here is the MTU handling of the network link. IPv6 ensures that the minimal link MTU of an IPv6 packet is 1280 bytes, while IPv4 uses packets with a minimal size of 68 bytes. When a translated IPv4 packet with a bigger MTU than 68 bytes arrives at an IPv4 router on a network with a minimal MTU of 68 bytes, the router fragments the translated IPv4 packet and forwards it over IPv4.

Network Address Translation and Protocol Translation (NAT-PT) is a transition mechanism to provide transparent routing between IPv4 and IPv6 end nodes. NAT-PT uses a combination of network address and protocol translation. The difference between NAT-PT and NAT in IPv4 is that translation does not happen between private and global addresses, but between IPv4 and IPv6 addresses.

Traditional NAT-PT With traditional NAT-PT, a host can only initiate a TCP (as well UDP and ICMP) session from the IPv6 network to connect an IPv4 host outside the network. These kinds of sessions are unidirectional. There are two variations of traditional NAT-PT, namely Basic NAT-PT and NAPT-PT.

Basic NAT-PTwith Basic NAT-PT a /96 prefix is reserved that can be routed in the IPv6 domain. All IPv6 traffic with the /96 destination prefix will be routed to the NAT-PT border router and translated to IPv4.

NAPT-PT stands for Network Address Port Translation and Protocol Translation and ex-tends the notion of translation one step further. NAPT-PT allows multiple IPv6 hosts to share a single IPv4 address to communicate transparently with the hosts outside the NAPT-PT router.NAPT-PT can be used in addition to basic NAT-PT to extend the pool of external map-ping addresses in conjunction with port translation. By assigning the TCP sessions from the initiating IPv6 hosts to ports in conjunction with IPv4 addresses, a maximum of 63000 TCP and 63000 UDP sessions per IPv4 are available to assign. There are 254 IPv4 addresses available, which are enough possibilities for address mapping.

Bidirectional NAT-PT combined with a DNS Application Layer Gateway provides bi-directional connectivity between an IPv6 domain and an IPv4 domain outside the NAT-PT border router. This mechanism employs the possibility to initiate TCP sessions from as well IPv6-only hosts as from an

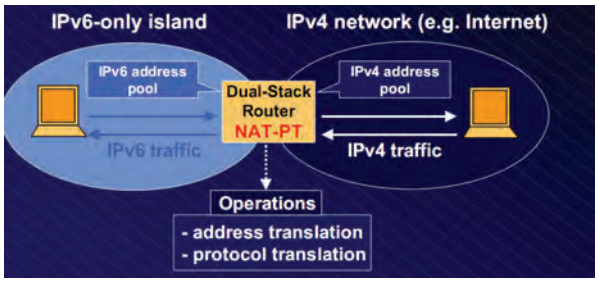

Fig 6. Dual-stack alternative

Issues with NAT-PT

- More or less the same as IPv4 NATs
- some applications may not work (need for ALGs)
- IPsec, Mobile IP, etc. fail (no e2e transparency)
- performance degradation
- single point of failure
- need for strict coordination with DNS for automatic translation state initialization

But unlike IPv4 NATs, NAT-PTs are just a temporary solution and after the transition has been completed the NAT-PT box may be removed

Transport Relay Translator- the transport relay translator (TRT) mechanism functions on the transport layer of the TCP/IP reference model. It allows IPv6-only nodes to communicate with IPv4-only nodes by translating TCP-over-IPv6 to TCP-over-IPv4, and the other way round. The TRT mechanism works the same for UDP track. The TRT system can be located on a dual stack host or router. When an initiating IPv6 host wants to communicate with an IPv4 host it needs an IPv6 destination address. All TCP traffic from the IPv6 host goes through the TRT system, which functions as a traffic relay server. When the TRT system receives incoming TCP traffic from an IPv6 source host (X6) to an IPv4 destination host (Y4), it makes an IPv6 connection with the initiating IPv6 host. The TRT system is configured with a dummy IPv6 prefix like C6::Y4/64, where Y4 is the destination IPv4 address. The initiating IPv6 host has the ability to connect to the IPv4 host through the IPv6 address C6::Y4.After that, the relay server makes a connection w the IPv4 host and forwards the TCP traffic to the IPv4 host. When the relay server receives traffic from the IPv4 host, it establish in the same way a virtual connection with address C6::/64, and forwards the traffic to the IPv6 host.

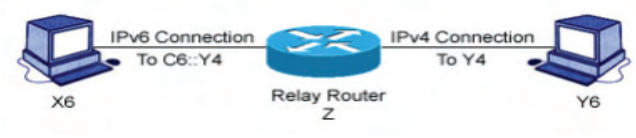

Fig 7. TRT Connection

Bump in the API- an alternative for the Bump in the Stack mechanism is the Bump in the API (BIA) mechanism. The main difference between the two is that BIA does not do any header translation, but performs its translation between the IPv4 API and IPv6 API on the application layer. The BIA API consists of three components, which are inserted between the socket API module and the TCP/IP module in a dual stack host. These components are: name resolver, address mapper, function mapper

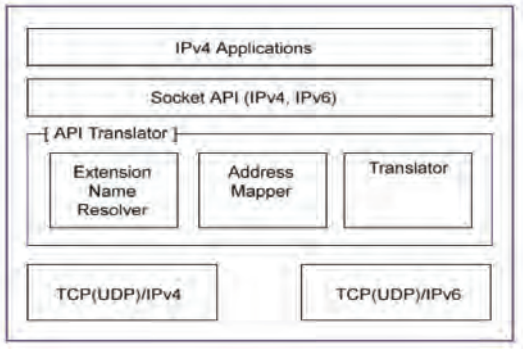

Fig 8. Architecture of the dual stack host using BIA

The name resolver and address mapper are the same as used in BIS. The main di erence between BIS en BIA happens in the translation function. The function mapper in BIA captures IPv4 socket API function calls and converts them to new IPv6 socket API function calls. BIA translates in the same way from IPv6 to IPv4.

V. Conclusion

We believe that running both protocol versions at the same time based on the dual stack approach while deploying IPv6 in phases, is the key to a successful IPv6 migration. IPv6 connectivity in a dual stack network environment means that current net-work security measures are not valid anymore for IPv6. Concerning viruses and worms, we don't expect these will be representing a potential IPv6 vulnerability since Antivirus software works independent of IPv4 or IPv6 unless the used software has been updated with IPv4 functionality.

VI. References

[1] Nordmark, "Stateless IP/ICMP Translation Algorithm (SIIT)", RFC 2765,
[2] February 2000.
[3] Tsirtsis and Srisuresh, "Network Address Translation - Protocol
[4] Translation (NAT-PT)", RFC 2766, February 2000.
[5] Tsuchiya, Higuchi and Atarashi, "Dual Stack hosts"
[6] Bump-in-the-Stack" technique (BIS)", RFC 2767, February 2000.
[7] Hagino and Yamamoto, "An IPv6-to-IPv4 Transport Relay Translator",
[8] IETF ipng working group http://www.ietf.org/html.charters/ipngwg-charter.html
[9] IETF ngtrans working group http://www.ietf.org/html.charters/ngtrans-charter.htm